CSE 227
Computer Security

Winter 2012

Stefan Savage

Course info

- Stefan Savage
  - Web: **http://www.cs.ucsd.edu/~savage**
  - E-mail: **savage@cs.ucsd.edu**
  - Office hours: M 3-4pm (or by appt, or drop by)
    CSE 3106
- Course Web pages (mostly empty now)
  - **http://www.cse.ucsd.edu/classes/wi12/cse227-a/**

This is a class “in progress”

You

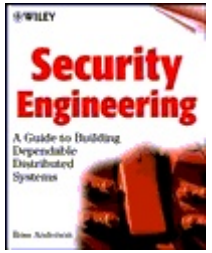
Me

Goals and non-goals

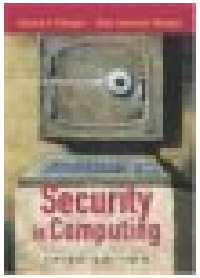
- Goals
  - Explore range of current problems and tensions in modern computer security
  - Understand how to identify security issues in your own research and how to address them
  - Figure out if security is an area of interest for you
  - Get feet wet in security research (mini research project)
- Non-goals
  - Review of all std security mechanisms
    - » Read a textbook or take CSE127
  - Significant examination of applied cryptography
    - » Take one of our great crypto courses

Readings

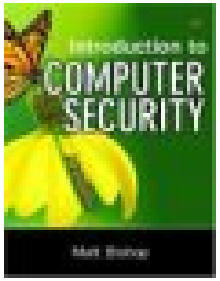
- There is **no textbook** for this class
  - We'll read a bunch of papers and occasionally from some books
- However, in general I recommend:
  - Security Engineering by Ross Anderson
    http://www.cl.cam.ac.uk/~rja14/book.html
    Second edition is better, but isn't free



- For those who want some general "backup", check out
  - *Security in Computing* by Charles Pfleeger



  - *Introduction to Computer Security* by Matt Bishop



Misc crud

- Grading (TBD)
  - Participation: xx%
  - Final (maybe?): yy%
  - Project: zz% (this will dominate.. whole purpose of class)

- **Research project**
  - Of your choosing (more on this Thurs)
  - Two people (if you want more, justify it to me)
  - Short paper (e.g. 6-8 pages) & presentation (10 mins)
  - High standards
    - » At least two papers published from class every year

My security background…

- Originally OS kernels…
  and networking…

- Came to Security by accident
  - Misbehaving TCP receivers – think like a bad guy
  - DDoS traceback – in response to 2000 attacks
- Startup
  and…

  synchronicity (David Moore @ UCSD found indirect evidence of spoofed DoS attacks, hmmm… general analysis possible)

  Startup was failure, analysis technique was golden
- Code Red
  - Same technique allowed measuring worm outbreaks
  - Interest * opportunity snowballed…

More Recently

- Research
  - I direct the Collaborative Center for Internet Epidemiology and Defenses (CCIED) (www.ccied.org)
    - » Joint UCSD/Berkeley ICSI effort
    - » Focus on large-scale Internet attacks (bots, spyware, worms)
    - » Particularly focused on the economics of Internet crime
  - Automotive security
  - Machine learning for security

Topics we'll be covering

- Human factors/usability
- Measurement/analysis studies
- System design/implementation
  - Protection, small TCB, etc
- Information exposure
  - Privacy, anonymity, side & covert channels
- Software vulnerabilities & malware
  - Vulnerability research, viruses, botnets, defenses, etc
- I'm open to more topics… got any?
- Some outside speakers

What is security?

What is security?

- Merriam-Webster online dictionary:

Function: *noun*

- ***Freedom from danger***
- ***Freedom from fear or anxiety***

the fulfillment of an obligation **b** : SURETY

3 : an instrument of investment in the form of a document (as a stock certificate or bond) providing evidence of its ownership

- ***Measures taken to guard against espionage or sabotage, crime, attack, or escape***

Computer security?

- Most of computer science is about providing functionality:
  - User Interface
  - Software Design
  - Algorithms
  - Operating Systems/Networking
  - Compilers/PL
  - Vision/graphics
  - Microarchitecture
  - VLSI/CAD

There are security problems in all of these domains

- Computer security is ***not*** about functionality
- It is about how the embodiment of functionality behaves in the presence of an adversary

Two competing philosophies...

- **Binary** model
  - Traditional crypto and trustworthy systems
  - Assume adversary limitations X and define security policy Y
  - If Y cannot be violated without needing X then system is secure, else insecure

- **Risk management** model
  - Most commercial software development (and much real-world security… e.g., terrorism)
  - Try to minimize biggest risks and threats
  - Improve security where most cost effective (expected value)

Classic example (binary): perfect substitution cipher

$$\begin{array}{ll} & p_1\ p_2\ p_3\ \ldots\ p_n \\ \oplus & b_1\ b_2\ b_3\ \ldots\ b_n \\ \hline & c_1\ c_2\ \ c_3\ \ldots\ c_n \end{array}$$

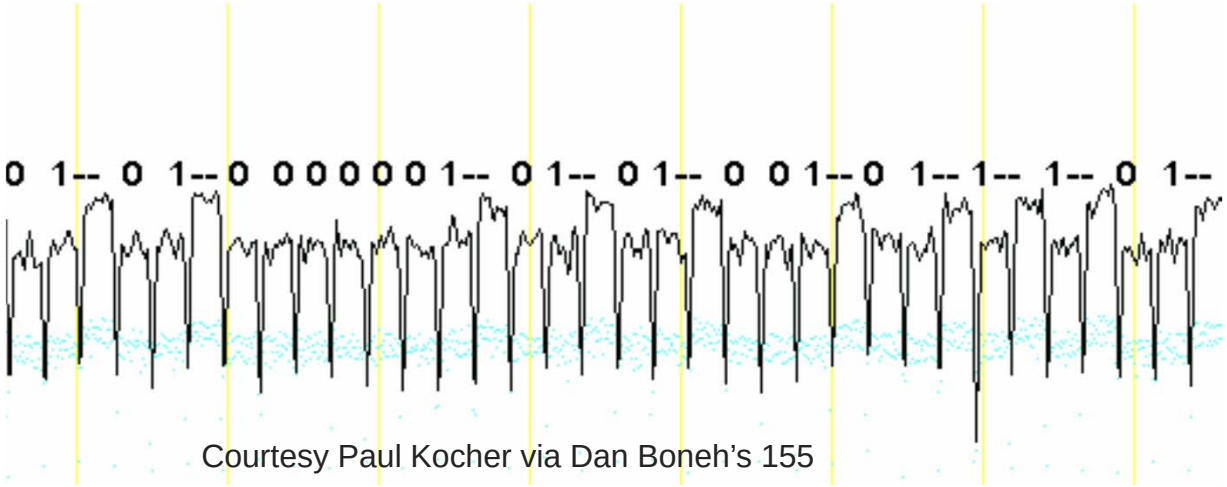
- Invited by combination of Vernam(1919) & Mauborgne
- Choose a string of random bits the same length as the plaintext, XOR them to obtain the ciphertext.
- Perfect Secrecy (proved by Claude Shannon)
  - Probability that a given message is encoded in the ciphertext is unaltered by knowledge of the ciphertext
  - Proof: Give me any plaintext message and any ciphertext and I can construct a key that will produce the ciphertext from the plaintext.

Classic example (risk mgmt): Concrete barricades

- Prevent incursion by car bombers

The problems with the binary model

- Hard to assume X in real systems
  - Real artifacts fragile, imperfect
    - » E.g. buffer overflow vulnerabilities
  - Implicit dependencies with exposed layer
    - » Example: reading RSA bits off current draw



Courtesy Paul Kocher via Dan Boneh's 155

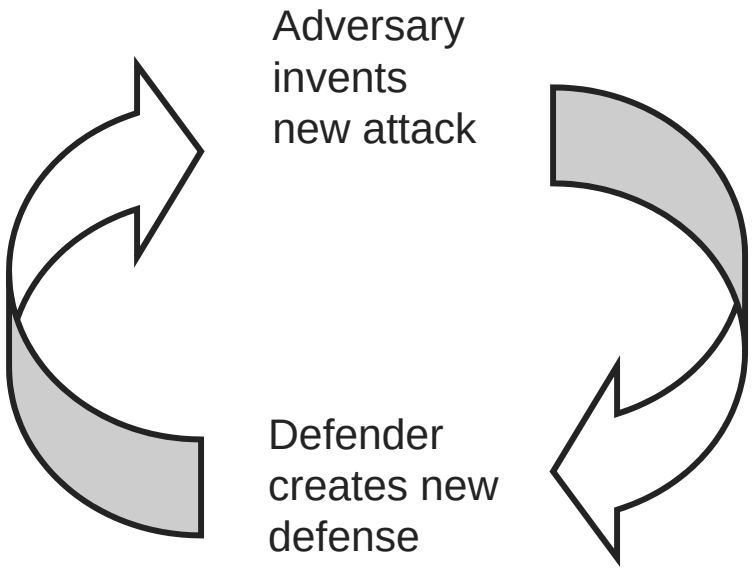
The problems with the binary model (cont)

- Hard to know what policy Y is in advance?
  - What are the dangers?
- Examples:
  - SPAM
  - Exchange rate fraud in South Africa vs SWIFT bank balance controls
  - Mobile code
- Finally: ***hugely expensive***… how many certified systems out there?

The problems with the risk management model

The problem with the risk management model

- Creates arms race – forced co-evolution



The problem with the risk management model

- Its fine to say security is a spectrum, but how to evaluate risk or reward?
  - How many quatloos of security does your anti-virus product give you?
- And the best you can hope for is stalemate
  - And we're losing stalemate in a number of situations (e.g., SPAM, Malware)

Key abstract security issues

- Risks
- Threats
- Value
- Protection (locks)
  - Confidentiality, integrity, authenticity, availability & access control
  - Policy
- Deterrence (police)
  - Non-repudiation, Accountability/Auditability
- Incentives
- Identity, reputation and due-diligence

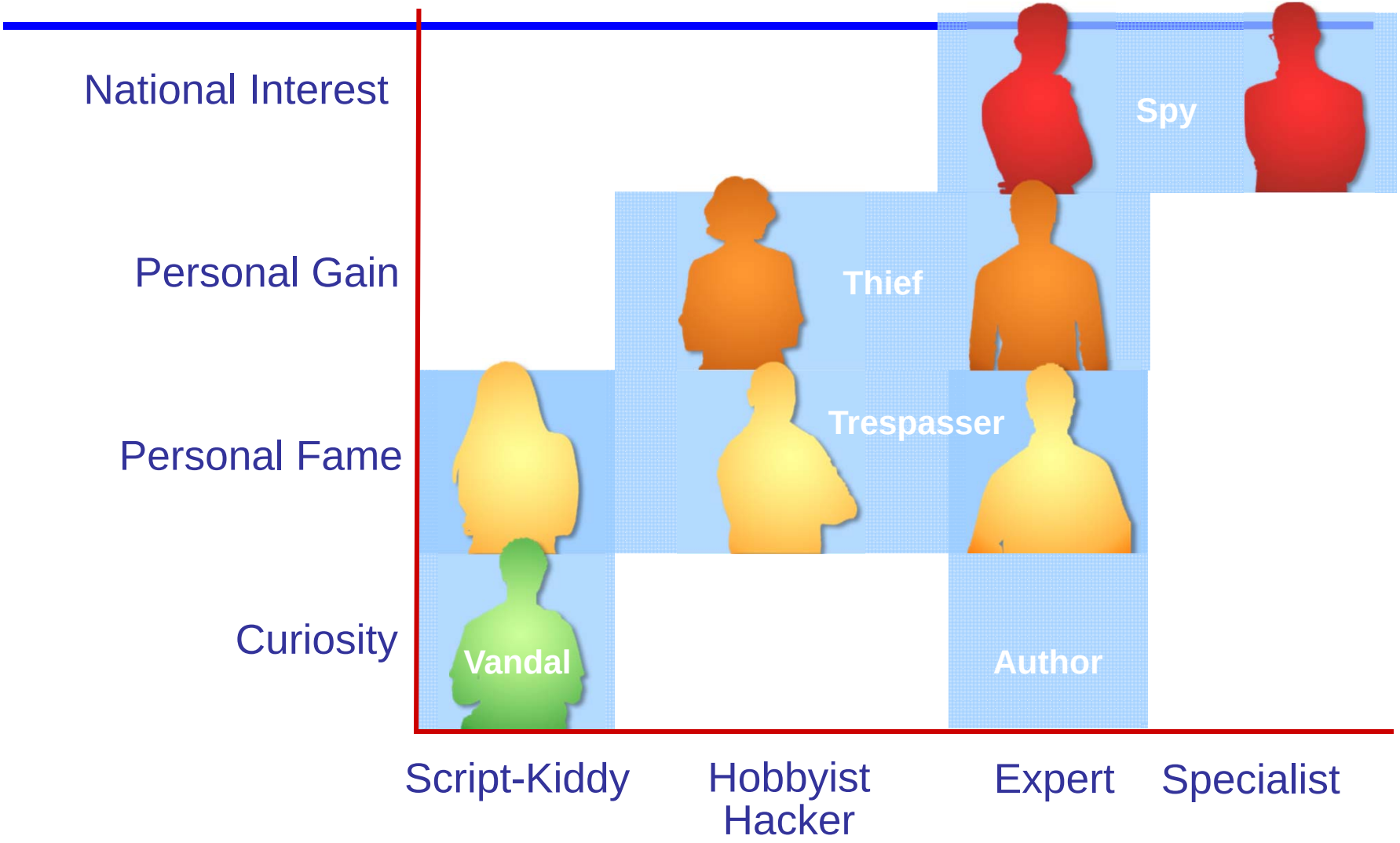
Risks & threats

- Risk
  - What bad things are possible?
  - How bad are they and how likely are they?
- Threats
  - Who is targeting the risk?
  - What are their capabilities?
  - What are their motivations?

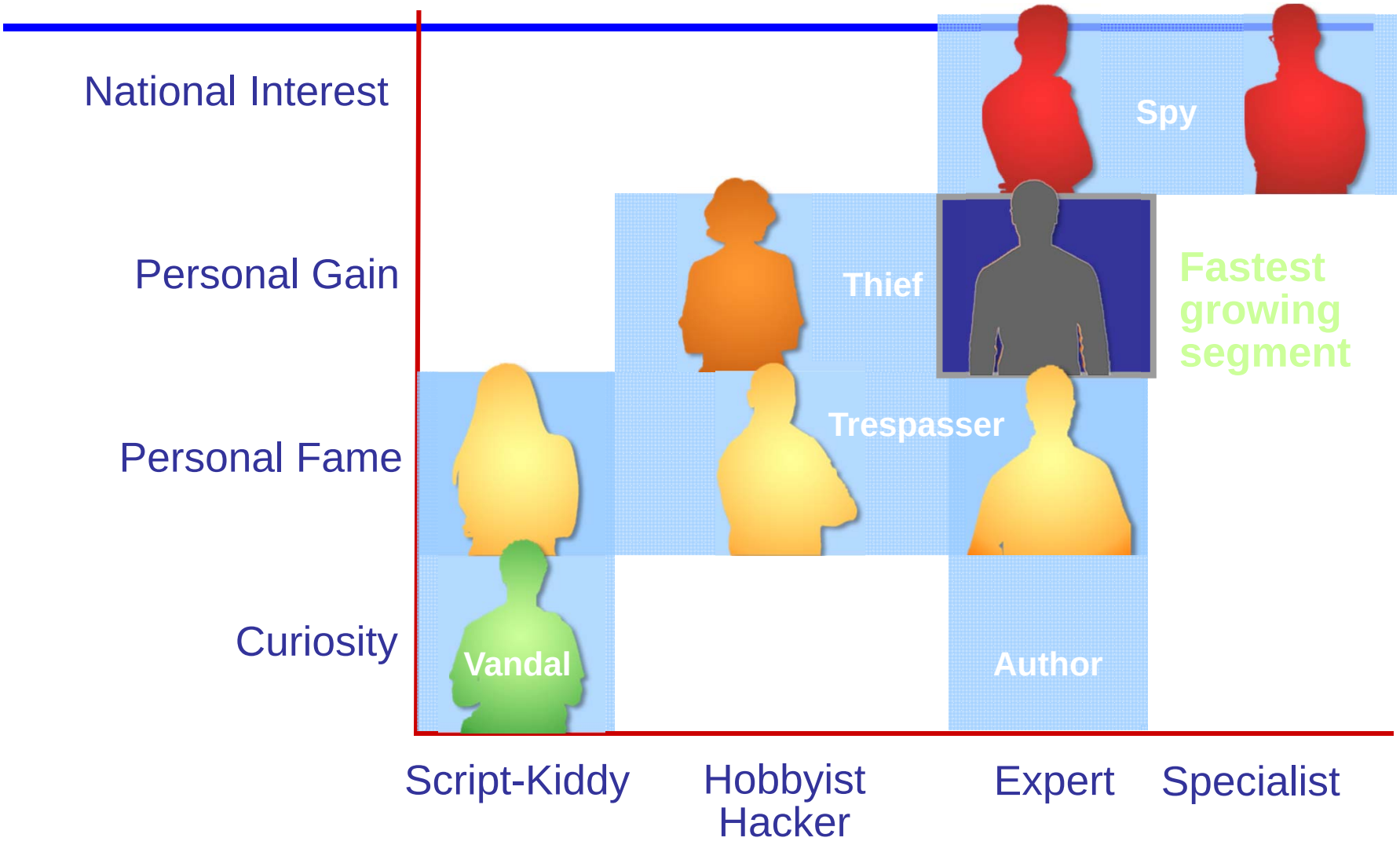
- These tend to be well understood/formalized in some communities (e.g. finance sector) and less in others (e.g. computer science)

The Threat Landscape

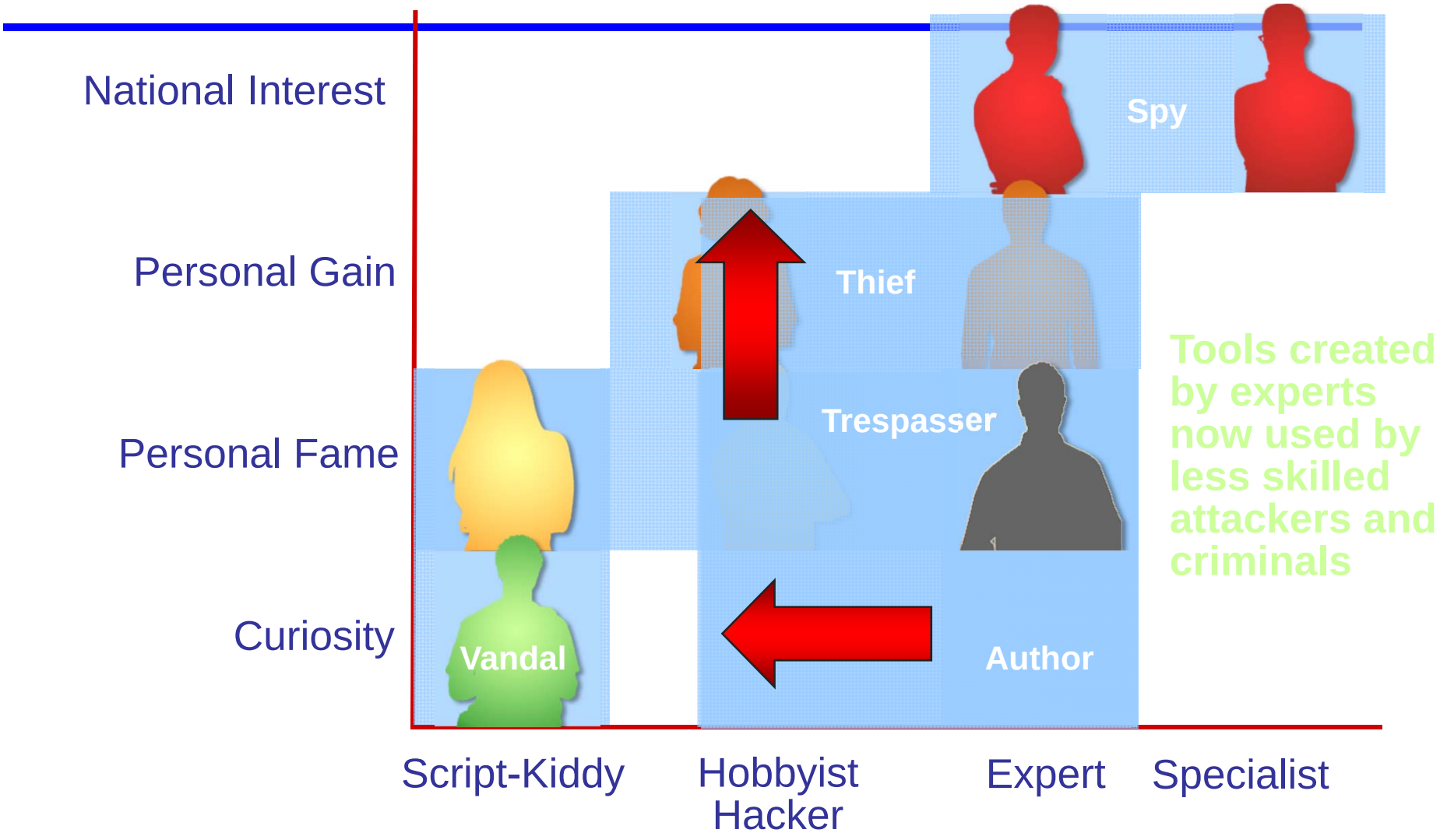
(courtesy David Aucsmith, Microsoft)



The Threat Landscape



The Threat Landscape



Value

- What is the cost if the bad thing happens?
- What is the cost of preventing the bad thing?

- Example: Visa/Mastercard fraud
- Example: Permission Action Links for nuclear weapons
  - http://www.cs.columbia.edu/~smb/nsam-160/pal.html

Protection (locks)

- The mechanisms used to protect resources against threats by enforcing some policy
  - This is most of academic and industrial computer security
- Many classes of protections
  - Cryptographic protection of data
  - Software guards
  - Communication guards
- Can be either proactive or reactive

Policy

- What **is** a bad thing?
- Remarkably tricky to define…
  - The software on your computer likely has 100s of security options
  - How should you set them?
- Can be non-intuitive
  - Should a highly privileged user have more rights on a system or less?

Deterrence

- There is some non-zero expectation that there is a future cost to doing a bad thing
  - i.e. going to jail, having a missile hit your house, having your assets seized, etc
  - Criminal cost-benefit: $M_b + P_b > O_{cp} + O_{cm}P_aP_c$ [Clark&Davis 95]
    - M_b : Monetary benefit
    - P_b : Psychological benefit
    - O_{cp} : Cost of committing crime
    - O_{cm} : Monetary cost of conviction
    - P_a : Probability of getting caught
    - P_c : Probability of conviction
- Need meaningful forensic capabilities
  - Audit actions, assign identity to evidence, etc
  - Must be cost effective relative to positive incentives

Incentives

- Factors that motivate a course of action

- Examples
  - Who pays for credit card theft?
  - What motivates vulnerability discovery?
  - What are the incentives for cyber crime prosecution?
  - What creates value in the security industry?

Identity & reputation

- What is identity?
  - Why is it valuable?
  - What's the difference between an identity and an identifier?

- Reputation?
  - Why is it valuable?
  - Relationship to identity? Identifier?
  - For what?

Difference between Due diligence and trust

- Due diligence
  - Work to acquire multiple independent pieces of evidence establishing identity/reputation linkage; particularly via direct experience
  - Expensive
- Trust
  - Allows cheap form of due-diligence: third-party attestation
  - Economics of third-party attestation? Cost vs limited liability
  - What is a third-party qualified to attest to?

That's it for today

- Any questions?
- For next time
  - I'm at Stanford
  - Stephen Checkoway will be talking about Car Security
- Read:
  - Both car security papers at autosec.org
    (both have pointers on the Web page)